MISSION NEED STATEMENT
for the
Security Assistance
Case Execution Management Information System (CEMIS)

1. Defense Planning Guidance (DPG) Element

1.1 Security Assistance does not fall within DPG Elements. However, the Security Assistance mission directly underwrites portions of the Secretary of Defense's (SECDEF's) "Security Cooperation Guidance" document of April 2003 and, in particular, the portion on "Strengthening Alliances for the Future". CEMIS also supports Goal 5 of the "Defense Security Cooperation Agency Strategic Plan 2003-2008". That goal is to "Identify and incorporate best business practices and deploy systems that save time, energy, and money".

1.2 Statutory requirements for Security Assistance primarily fall under the Foreign Assistance Act (FAA) of 1961, as amended and the Arms Export Control Act (AECA) of 1976, as amended.

1.3 The Security Assistance mission directly relates to the Office of the Under Secretary of Defense for Policy (OUSD(P)), Assistant Secretary of Defense (ASD) for International Security Affairs (ISA) and to strategic planning goals of that organization. The Defense Security Cooperation Agency (DSCA) is established under OUSD(P) and receives policy direction from the ASD(ISA). The Director, DSCA, will serve as both the Acquisition Milestone Decision Authority and the functional proponent of this system. CEMIS supports a culture of continuous improvement through Business Process Reengineering (BPR) and implementation of Foreign Military Sales (FMS) Reinvention Initiatives. Additionally, CEMIS will address the DSCA objective of formulating and executing an effective and affordable plan for the evolution of information systems supporting security cooperation business processes.

1.4 CEMIS is being funded from the FMS Administrative Trust Fund. The FMS fund is not Department of Defense (DoD) appropriated money, but rather money paid by the International Customers as a surcharge to administer their FMS cases.

1.5 CEMIS will respond to the requirements of the Clinger-Cohen Act through its reengineered approach to funds distribution and accountability. As a feeder system to Military Department (MILDEP) core accounting systems, CEMIS will include internal controls and financial reporting as specified in "A Guide to Federal Requirements for Financial Management Systems". This will permit the Security Cooperation community to be fully compliant with the statutory requirements of the Federal Financial Management Improvement Act (FFMIA) - which includes both the Federal Managers Financial Integrity Act (FMFIA) and Chief Financial Officer (CFO) Act.

1.6 This Mission Need Statement (MNS) was fully coordinated with each MILDEP and Defense Logistics Agency (DLA) members of the CEMIS Senior Steering Group and the Policy Program Group. DSCA memorandum 12 Jun 01 substantiated this coordination, and also provided copies of the MNS to the members.

2. Mission and Threat Analysis

2.1 Mission

2.1.1 The case execution process is the core of the Security Assistance mission. It is the logistics business process and accompanying financial business process that supports the sale, lease or grant of defense articles and services to foreign countries and international organizations. Since FMS is inherently a government-to-government affair, an element of the U.S. Government must manage the FMS program. By DoD Directive 5105.65, that element is DSCA. Detailed execution of the FMS program is conducted by each MILDEP under DSCA direction using joint automation services provided by DSCA.

2.1.2 Security Assistance is both a tool of foreign policy, and a large business. It is the sale, lease, or grant of defense articles or defense services to foreign countries and international organizations. The sales average approximately $12 billion per year, which places Security Assistance in the category of a major business. During an average year, Security Assistance can have approximately $225B of total case value in open FMS cases that are being managed - representing a span of over 180 different countries, multiple military services or agencies within each country, and various international organizations.

2.1.3 A key requirement of selling in the international market is customer satisfaction. This challenge is heightened by the ever-increasing desire of the international customers for transparency into our processes, and having access to information. Each country, and each military service or agency within that country has its own specific level of requirements related to information concerning their equipment, delivery, status of payment etc. To meet customer satisfaction - in being good stewards of their money, while ensuring timely and accurate delivery of their purchase - requires an increasing need for fidelity and accuracy in our automated information systems that we do not currently have.

2.1.4 The current unclassified independent (single service) case execution information systems are:

- The Centralized Integrated System for International Logistics (CISIL) – Army
- The Management Information System for International Logistics (MISIL) – Navy
- The Security Assistance Management Information System (SAMIS) - Air Force
- The Case Management Control System (CMCS) - Air Force.

2.1.5 This Mission Need Statement (MNS) focuses on the third phase (case execution) of the Security Assistance process but also will incorporate the fourth phase (case closure).

2.1.6 The principal case execution functions of DSCA include administering and supervising security assistance planning and programs, coordinating the formulation and execution of security assistance programs with other governmental agencies, developing and operating the data processing systems, and maintaining macro databases for the security assistance program. Business is conducted on a U.S. Government-to-International Government basis, and cannot be performed by private industry or another government organization.

2.1.7 Globalization and defense transformation has made the foreign policy aspect of the Security Assistance mission increasingly complex. An advanced level of automated information systems (AIS) is required in order to respond quickly and accurately with country, regional, and global

information within the Office of the Secretary of Defense, to the Department of State, and to Congress. It is also the big business aspect of selling to an international market that requires a level of AIS that is currently not available to the Security Assistance community. Our international customers require a similar quick and accurate response on the status of their country's purchases and their financial payments. Our Security Assistance managers also need similar advanced AIS support in order to effectively meet our mission.

2.2 Threat

2.2.1 CEMIS is an information system susceptible to computer network attack, electronic warfare, denial and deception, and physical attack. Each of these measures poses a threat to CEMIS. The projected threat environment in which the CEMIS will operate includes an established and continually growing number of world wide entities capable of conducting information operations (IO). Some subsets of these most likely have specific tasking against U.S. communications, networks, and computer systems. Computer network attack threat mechanisms are grouped into four categories: Compromise-of-information, Data Deception or Corruption, Information denial or loss, and Physical Destruction or Damage. These systems face threats that are genuine, worldwide in origin, technically diverse, multifaceted, and growing rapidly. The detailed threat environment for information systems is described in the following Defense Intelligence Agency (DIA) validated publications: Automated Information System Threat Environment Description (U), NAIC-1574-0210-00 September 2000 (S//NF), and Electronic Warfare Threat Environment Description (U), NAIC-1574-0731-01, February 2001 (S//NF).

2.2.2 CEMIS is a business system and needn't be designed for nuclear, chemical, or biological operations. Normal DoD data processing protections will be sufficient. The dominant threats are external and internal hackers and natural disasters. A unique threat to CEMIS will be the presence of foreign customer users whose nations may be one another's enemies. This requires an ability to reliably segregate data by nation when used by foreign customers.

2.3 Current Deficiencies -- Shortfalls

2.3.1 DSCA published a Deficiency Analysis on 19 Apr 01 that was prepared in conjunction with the Military Departments and International Customer representatives. Members of the Security Assistance community analyzed and identified key deficiencies in the current legacy systems that are related to specific tasks in the case execution process needing to be corrected

2.3.2 Each foreign military sale is called a "case" that flows through four phases:

- Development (the request from the country and the U.S. approval process)
- Implementation (when the case is signed and funds are initially provided)
- Execution (the ordering and shipment of U.S. defense articles to the foreign country, or the performance of defense services)
- Closure (when all items and services have been shipped or performed, and there is a final statement of account).

2.3.3 The legacy case execution systems:

- Contain many redundant processes and information.
- Produce inconsistent results.
- Have complex user interfaces that are difficult to learn.
- Have multiple interfaces with other DoD systems, which can require major reconciliation efforts.
- Contain nonstandard data element definitions which lead to confusion for all major stakeholders, including the International Customers.
- Have limited ad hoc reporting capability.
- Present a single-service view, which seriously hinders requirements for a tri-service and customer-oriented view.
- Have been identified as critical feeder systems and are not currently compliant with the Chief Financial Officer (CFO) Act, or the Federal Manager's Financial Integrity Act (FMFIA).
- Are not compliant with DoD Electronic Data Interchange (EDI) Standards.

2.3.4 Existing case execution information systems are aging, expensive to maintain, and do not meet many current user requirements. These requirements include providing timely and accurate tri-service multi-country information, not only to various offices within the Department of Defense, the Department of State, and Congress for key decision-making, but also to our own Security Assistance leaders for more effective management in support of our mission. The requirements also include satisfying the information needs of the International Customer in an increasingly complex global environment.

2.3.5 These legacy systems, as well as the one classified system, called the 1200 System, were built to adequately meet requirements existing at the time; however, they do not meet current multi-user requirements. Nor do they provide the ability to meet international customer satisfaction. This lack of modern AIS diminishes our ability to perform the Security Assistance case execution mission today - and in the future.

2.3.6 Any future systems development/enhancement efforts should be aimed at reducing the man-years of effort required for system maintenance, and reducing the expense of hardware platforms housing the system, without diminishing user accessibility to the system or the speed at which information is retrieved.

2.3.7 Unique Security Assistance business processes and reports need to be reengineered and standardized across DoD. The most cost-effective methods need to be institutionalized for this effort, rather than making duplicate efforts in each separate system.

3. Non-Materiel Alternatives

No doctrinal, operational concept, organizational, or training changes will eliminate or moderate this need.

4. Potential Materiel Alternatives

4.1 HQ DSCA has several materiel alternatives from which to select a course of action that meets the business and financials goals of the Security Assistance community. Consistent with DoD policy, the commercial software marketplace will be examined to assess whether adequate fit and adoption of commercial practices can satisfy the Security Assistance mission. A rigorous analysis of alternatives will be conducted to explore the feasibility, costs, and projected schedule to achieve a core level of Security Assistance information management. HQ DSCA will establish a baseline definition of functionality by providing funds to each Security Assistance component and establishing DoD-wide working groups for the purpose of business process reengineering and reports standardization.

4.2 The reengineered business processes are likely to be implemented in several phases. Hence, the alternatives will consider an evolutionary approach to developing a system that incrementally achieves the benefits of the new business processes consistent with the investment required to implement them. The evolutionary approach will allow HQ DSCA to better react to the ever-changing information needs and take advantage of evolving information management technologies.

4.3 There is a range of alternatives that may satisfy the information management needs of the Security Assistance community. Consistent with HQ DSCA Strategic Plan objectives and DoD acquisition policies, HQ DSCA choices include, but are not limited to, the following alternatives. Specifically, HQ DSCA may:

- Choose the best existing system or subsystem for each group of business processes and reengineer, standardize, and modernize as appropriate.
- Choose to fully construct a new system and migrate legacy data to that new system.
- Choose to evolve each of the legacy systems for another few years, and provide enough time to fully construct a new system and migrate legacy data to that new system.
- Choose an approach that would provide a portal technology to provide tri-service views/reports, maintaining tri-service data in a data warehouse, and modernize the background legacy systems or build a new background system.
- Acquire and integrate one or more commercial off-the-shelf (COTS) products.
- Choose from other options that may become defined during Concept Exploration.

5. Constraints

5.1 Objectives

The Case Execution Management Information System (CEMIS) must:

- Be quick, efficient, reliable, and user-friendly.
- Provide timely and accurate data.
- Uniformly store and report information so that there will be increased tri-service compatibility.
- Have ad hoc reporting capability.
- Satisfy DoD requirements and meet International Customer needs.
- Be able to support at least 2,000-5,000 concurrent users at more than 250 user sites.

- Be able to process a minimum of 250,000 batch transactions and 400,000 interactive transactions per day.
- Be able to perform all Security Assistance business processes and interfaces, and produce all required documents and reports.
- Have an ad hoc reporting capability that is flexible, efficient and user friendly.
- Have an interactive response time of 3 to 5 seconds or faster on all but the most complex screen entries.

5.2 Classification Level

CEMIS must be unclassified to allow interface with other DoD systems, to allow use by the international customers, and to accommodate the vast majority of FMS cases. However, one country's data must be protected from another country's view. CEMIS must meet the security requirements of DoD Directive 5200.28 “Security Requirements for Automated Information Systems (AIS)”, and the accreditation requirements of DoD Instruction 5200.40 “DoD Information Technology Security Certification and Accreditation Process (DITSCAP)”. A separate system, as a replacement for the current classified system (the 1200 System), will be required to handle the classified data outside of the CEMIS program.

5.3 Compliance Requirements

CEMIS must be compliant with all applicable DoD Security Assistance, financial, logistics, acquisition, and information technology regulations. CEMIS must be compliant with the Chief Financial Officer (CFO) Act, the Federal Manager’s Financial Integrity Act (FMFIA), and OMB Circular A-130 “Management of Federal Information Resources”. CEMIS must also be compliant with DoD Directive 8190.1 “DoD Logistic Use of Electronic Data Interchange (EDI) Standards”. CEMIS is also intended to be compliant with the Global Information Grid (GIG) architecture and meet the GIG Key Performance Parameters and to comply with the standards of DoD Joint Technical Architecture (JTA). Of particular importance is GIG Capstone Requirements Document requirement IV.B.2.p for non-GIG interoperability to allow data access by foreign customers.

5.4 Infrastructure Requirements

5.4.1 Any new systems development should incorporate Commercial Off-the-Shelf (COTS) software packages where possible to reduce overall costs. A modern software development environment and a modern database management system must be used, with complete documentation and be a highly flexible system in order to reduce future man-year maintenance costs.

5.4.2 As regards the National Supply System (NSS) and Information Technology Services (ITS) support, CEMIS will not employ tactical or deployable communications. It will operate as one or more applications in a DISA Defense Enterprise Computing Center, possibly in a DISA Demilitarized Zone (DMZ). It will require Non-Secure Internet Protocol Router (NIPRNET) usage and usage of the commercial internet.

5.4.3 System design shall promote human performance and Manpower, Personnel, and Training (MPT) efficiencies to the greatest extent possible.

5.5 Operating Environment

5.5.1 CEMIS must be capable of interoperating with the DoD communications infrastructure and be able to interface with all implementing agencies and their domestic logistics, acquisition, financial, or Enterprise Resource Planning (ERP) systems. It must also be capable of interoperating with commercial infrastructure as required to allow International Customer access. CEMIS must also be able to interface with other Security Assistance systems such as the Defense Integrated Financial System (DIFS) and the Defense Security Assistance Management System (DSAMS), as well as the worldwide Security Assistance community.

5.5.2 CEMIS must economize in use of bandwidth since many customers and Security Assistance Offices (SAOs) have austere dial-up communications. If a web-based approach is employed, screens should be design with minimal graphics. From a supportability perspective, it is desirable to avoid custom client software since it requires approval and installation by Local Area Network (LAN) administrators in over 100 countries. While it should be an objective to reduce the software maintenance costs of CEMIS compared to that of the legacy systems, the Analysis of Alternatives allows for options in which this may not occur. CEMIS will not employ tactical or mobile communications. As a user of common-user data communications systems, it will have no unique signature.

5.5.3 FMS customers will have access to CEMIS data. However, the software will be retained by DSCA. No non-U.S. citizen or dual citizenship personnel will be involved in system development.

6. Joint Potential Designator

Joint Interest.